Windows Authentication Issue



Unable to do Windows Authentication while accessing the Application.

Y Solution

Below is the configuration setting on the Server related to Windows Authentication.

Section: system.webServer/security/authentication/windowsAuthentication

· From: ApplicationHost.config <location path='UAT-WFE-

Deepest Path: MACHINE/WEBROOT/APPHOST/UAT-WFE-SGP							
authPersistNonNTLM	True						
authPersistSingleRequest	False						
enabled	False						
extendedProtection							
providers	(Count=2)						
useAppPoolCredentials	False						
useKernelMode	True						

authPersistNo Optional Boolean attribute.								
nNTLM								
	Specifies whether IIS automatically reauthenticates every non-NTLM (for example, Kerberos) request, even those on the same connection. False enables multiple authentications for the same connections.							
	Note: A setting of true means that the client will be authenticated only once on the same connection. IIS will cache a token or ticket on the server for a TCP session that stays established.							
	The default is false.							
authPersistSi	Optional Boolean attribute.							
ngleRequest								
	Setting this flag to true specifies that authentication persists only for a single request on a connection. IIS resets the authentication at the end of each request, and forces reauthentication on the next request of the session.							
	readmentication on the next request of the session.							

Configuration on the APV was not compatible with above mentioned Settings on the Application and due to this Users were not able to do Authentication or not able to access the application properly.

With Default configuration on APV: i.e. having "HTTP Authsplice on <Virtual Service>" CLI, Server was authenticating the Users, however, subsequent request after the Login were being forwarded to same server and this was creating an issue.

Because, for all the initial requests, Server was Responding with HTTP Response "401 unauthorized" and due to this, APV thinks that, all the requests from the Client may require Authentication and will be forwarded to same server without going into SLB lookup (Checking the Policies or Group Methods) Process.

Due to this, users were not able to access the Subsequent requests post login or Authentication.

Hence In order to fix this, we were supposed to disable the "http authsplice off <virtual Service>".

However, Post making this, users were not able to login into application as "APV was using different TCP connections" to forward the Authentication requests (Request, NTLMSSP-Negotiate, NTLMSSP-Auth) to Servers and Server was unable to Authenticate it.

But in the case of "http authsplice on <virtual Service>", APV was using single TCP connection to complete all the Authentication requests (Request, NTLMSSP-Negotiate, NTLMSSP-Auth). To fix this we have disabled the "Connection Reuse" on the Real Server.

Final configuration on APV to make it compatible with Application access and Windows Authentication is,

- Keeping HTTP AuthSplice to off on Virtual Service
- Disabling Connection Reuse on Real Servers.

Command to disable Authsplice

http authsplice {on|off} <virtual_service>

Command to disable Connection Reuse on Real Server

http serverconnreuse real <real_service> off

Below is the screenshot when Connection Reuse is off on RS and AuthSplice off on VS.

Seesion-ReUse-Off-Auth-Off-LB-Working.pcap - 🗇										
<u>F</u> ile <u>E</u> dit	t <u>V</u> iew	<u>Go</u> <u>C</u> ap	oture <u>A</u>	nalyze <u>S</u> tatisti	cs Telephon	y <u>W</u> ireless	<u>T</u> ools <u>H</u> elp			
		🔚 🔀	C 9	⇔ ⇒ 😤 👔	5 J. 🔳 🗄	= e e (Ð. 111			
						_	•			
http://stforwarded_for == "172.17.0.204"										
Destinat	tion	Protocol	Length	Time : X-Forward	ded-For		802.1 Source	Pc Destination	Port Stream Info	
4 10.10.	.12.129	HTTP	685	129.126	5.162.82,17	2.17.0.204	4760	L 80	25 GET / HTTP/1.1	
4 10.10.	.12.129	HTTP	894	129.126	5.162.82,17	2.17.0.204	4760	L 80	25 GET / HTTP/1.1 , NTLMSSP_NEGOTIATE	
4 10.10.	.12.129	HTTP	1102	129.126	5.162.82,17	2.17.0.204	4760	L 80	25 GET / HTTP/1.1 , NTLMSSP_AUTH, User: DIRECTASIA\jeng	
4 10.10.	.12.129	HTTP	863	129.126	5.162.82,17	2.17.0.204	4760	L 80	25 GET / HTTP/1.1	
	.12.129	HTTP	946	129.126	5.162.82,17	2.17.0.204	4760		25 GET / HTTP/1.1 , NTLMSSP_NEGOTIATE	
	.12.129	HTTP	1146			2.17.0.204			25 GET / HTTP/1.1 , NTLMSSP_AUTH, User: \UAT_testuser	
4 10.10.	.12.129	HTTP	757	129.126	5.162.82,17	2.17.0.204	4760	L 80	25 GET /ruxitagentjs_ICA27SVfqrux_10185200219132536.js HTTP/1.1	
	.12.129	HTTP	988			2.17.0.204	4760		25 GET /assets/fonts/Montserrat/Montserrat-Regular.ttf HTTP/1.1	
	.12.129	HTTP	1071	129.126	5.162.82,17	2.17.0.204			25 GET /assets/fonts/Montserrat/Montserrat-Regular.ttf HTTP/1.1 , NTLMSSP_NEGOTIATE	
	.12.129	HTTP	1271			2.17.0.204			25 GET /assets/fonts/Montserrat/Montserrat-Regular.ttf HTTP/1.1 , NTLMSSP_AUTH, User: \UAT_to	
	.12.129	HTTP	938		5.162.82,17	2.17.0.204			25 GET /assets/image/directasia-ins.png HTTP/1.1	
	.12.129	HTTP	1021	129.126	5.162.82,17	2.17.0.204	4760		25 GET /assets/image/directasia-ins.png HTTP/1.1 , NTLMSSP_NEGOTIATE	
	.12.129	HTTP	1221			2.17.0.204			25 GET /assets/image/directasia-ins.png HTTP/1.1 , NTLMSSP AUTH, User: \UAT testuser	
	.12.129	HTTP	1186	129.126	5.162.82,17	2.17.0.204			25 GET /app/ui/js/marketingtracking/qualaroo/common.qualaroo.html HTTP/1.1	
	.12.129	HTTP	1269			2.17.0.204	4760		25 GET /app/ui/js/marketingtracking/qualaroo/common.qualaroo.html HTTP/1.1 , NTLMSSP_NEGOTIA	
	.12.129	HTTP	1470	129.126	5.162.82,17	2.17.0.204	4760	1 80	25 GET /app/ui/js/marketingtracking/qualaroo/common.qualaroo.html HTTP/1.1 , NTLMSSP_AUTH, U	
	.12.129	HTTP	1083	129.126	5.162.82,17	2.17.0.204			25 GET /assets/image/svg-icons/ico_policyholder_reverse.svg HTTP/1.1	
	.12.129	HTTP	1166			2.17.0.204	4760		25 GET /assets/image/svg-icons/ico_policyholder_reverse.svg HTTP/1.1 , NTLMSSP_NEGOTIATE	
	.12.129	HTTP	1366			2.17.0.204			25 GET /assets/image/svg-icons/ico_policyholder_reverse.svg HTTP/1.1 , NTLMSSP_AUTH, User: \I	
	.12.129	HTTP	1064			2.17.0.204			25 GET /assets/image/svg-icons/Email.svg HTTP/1.1	
	.12.129	HTTP	1147			2.17.0.204	4760		25 GET /assets/image/svg-icons/Email.svg HTTP/1.1 , NTLMSSP_NEGOTIATE	
	.12.129	HTTP	1347			2.17.0.204			25 GET /assets/image/svg-icons/Email.svg HTTP/1.1 , NTLMSSP_AUTH, User: \UAT_testuser	
	.12.129	HTTP	761			2.17.0.204			47 GET /assets/css/bundle.min.css?v=20192708 HTTP/1.1	
	.12.129	HTTP	844			2.17.0.204	2437		47 GET /assets/css/bundle.min.css?v=20192708 HTTP/1.1 , NTLMSSP_NEGOTIATE	
4 10.10.	.12.129	HTTP	1044	129.126	5.162.82,17	2.17.0.204	2437	2 80	47 GET /assets/css/bundle.min.css?v=20192708 HTTP/1.1 , NTLMSSP AUTH, User: \UAT testuser	

Below is the screenshot when Connection Reuse is ON on RS and AuthSplice off on VS. 【B_Auth-Off.pcap File Edit View Go Capture Analyze Statistics Telephony Wireless Iools Help

<u>F</u> ile <u>E</u> dit <u>V</u> i	ew <u>G</u> o <u>C</u> apture	<u>A</u> nalyze	<u>Statistics</u> Te	lephon <u>y</u> <u>W</u> ireless	<u>T</u> ools <u>H</u> elp				
🥖 🔳 🙇 🔘	- 🔚 🔀 🖨	ې 🗢 ک	😤 👔 👃	📃 📃 🔍 🔍	Q. 🎹				
http.x_forwa	rded_for == "10.20.30	.235"							Expression
Source	Destination	Protocol	Length Time	x-Forwarded-For	802.1 Source Po	Destination Port	Strear Info		
. 172.17.1.2	04 10.10.12.129	HTTP	553	10.20.30.235	15900	80	44 GET / HTTP/1.1		
172.17.1.2	04 10.10.12.129	HTTP	762	10.20.30.235	15900	80	44 GET / HTTP/1.1 ,	NTLMSSP NEGOTIATE	
172.17.1.2	04 10.10.12.129	HTTP	970	10.20.30.235	15900	80	44 GET / HTTP/1.1 ,	NTLMSSP AUTH, User: DIRECTASIA\jeng	
172.17.1.2	04 10.10.12.129	HTTP	705	10.20.30.235	15900	80	44 GET / HTTP/1.1		
172.17.1.2	04 10.10.12.129	HTTP	788	10.20.30.235	15900	80	44 GET / HTTP/1.1 ,	NTLMSSP_NEGOTIATE	
172.17.1.2	04 10.10.12.129	HTTP	988	10.20.30.235	15900	80	44 GET / HTTP/1.1 ,	NTLMSSP_AUTH, User: \UAT_testuser	
172.17.1.2	04 10.10.12.129	HTTP	614	10.20.30.235	15900	80	44 GET /ruxitagentjs	_ICA275Vfqrux_10185200219132536.js HTTP	/1.1
172.17.1.2	04 10.10.12.129	HTTP	581	10.20.30.235	15900	80	44 GET /assets/lib.j	s HTTP/1.1	
172.17.1.2	04 10.10.12.129	HTTP	619	10.20.30.235	36515	80	80 GET /assets/css/b	undle.min.css?v=20192708 HTTP/1.1	
172.17.1.2	04 10.10.12.129	HTTP	595	10.20.30.235	36517	80	81 GET /assets/confi	g/config.min.js HTTP/1.1	
172.17.1.2	04 10.10.12.129	HTTP	848	10.20.30.235	36517	80	81 GET /assets/confi	g/config.min.js HTTP/1.1 , NTLMSSP_NEGO	TIATE
. 172.17.1.2	04 10.10.12.129	HTTP	1072	10.20.30.235	36517	80	81 GET /assets/css/b	undle.min.css?v=20192708 HTTP/1.1 , NTL	MSSP_AUTH, User: \UAT_testuser
172.17.1.2	04 10.10.12.129	HTTP	861	10.20.30.235	36517	80	81 GET /assets/lib/m	arketingtracking/tabletop.js HTTP/1.1 ,	NTLMSSP_NEGOTIATE
172.17.1.2	04 10.10.12.129	HTTP	1061	10.20.30.235	36517	80	81 GET /assets/lib/m	arketingtracking/tabletop.js HTTP/1.1 ,	NTLMSSP AUTH, User: \UAT testuser
172.17.1.2	04 10.10.12.129	HTTP	848	10.20.30.235	36517	80	81 GET /assets/confi	g/config.min.js HTTP/1.1 , NTLMSSP_NEGO	TIATE
. 172.17.1.2	<u>04 10.10</u> .12.129	HTTP	872	10.20.30.235	36517	80	81 GFT /assets/css/b	undle.min.css?v=20192708 HTTP/1.1 . NTL	MSSP_NEGOTTATE
LB_Auth-O	f.pcap								-
<u>F</u> ile <u>E</u> dit <u>\</u>	iew <u>G</u> o <u>C</u> apture	<u>A</u> nalyze	Statistics	Telephon <u>y</u> <u>W</u> irele	ss <u>T</u> ools <u>H</u> elp				
<u> </u>) 📙 🛅 🔀 🖸	ې 🗢 🖻	> 🕾 🚹 🛓	<u>}</u>	Q 🔍 🎹				
http.request	.uri == "/assets/lib.js"	and http.x_f	orwarded_for	== "10.20.30.235"					Ext
No. 1	ime Source	De	stination	Protocol Lengt	Time : X-Forwarde	d-For 802	1 Source Po Destination Port	Streai Info	
797 @	6:39:0 172.17.	1.204 10	.10.12.129	HTTP 58	1 10.20.30	.235	15900 80	44 GET /assets/lib.js HTTP/1.1	
→ 1207 0	6:39:0 172.17.	1.204 10	.10.12.129	HTTP 83	4 10.20.30	.235	15908 80	82 GET /assets/lib.js HTTP/1.1 , NTLM	ISSP_NEGOTIATE
1263 0	6:39:0 172.17.	1.204 10	.10.12.129	HTTP 104	2 10.20.30	.235	15908 80	82 GET /assets/lib.js HTTP/1.1 , NTLM	AUTH, User: DIRECTASIA\jeng
945 0	6:39:0 172.17.	1.204 10	.10.12.129	HTTP 83	4 10.20.30	.235	15910 80	84 GET /assets/lib.js HTTP/1.1 , NTLM	ISSP_NEGOTIATE
1062 0	6:39:0 172.17.	1.204 10	.10.12.129	HTTP 103	4 10.20.30	.235	15910 80	84 GET /assets/lib.js HTTP/1.1 , NTLM	ISSP_AUTH, User: \UAT_testuser

٥

Below is the screenshot when Connection Reuse is ON on RS and AuthSplice ON on VS.

Auth-ON_L8.Pcap

Ele Edit View Go Capture Analyze Statistics Telephony Wireless Jools Help

- [📕 http://greaded_for == "10.20.30.235"										
	Source	Destination	Protocol	Length Ti	me : X-Forwarded-For	802.1 Source Po	Destin S	itream index Info			
	_ 172.17.1.	204 10.10.12.129	HTTP	553	10.20.30.235	16198	80	38 GET / HTTP/1.1			
	_ 172.17.1.	284 10.10.12.129	HTTP	762	10.20.30.235	16198	88	38 GET / HTTP/1.1 , NTLMSSP_NEGOTIATE			
	. 172.17.1.	284 10.10.12.129	HTTP	978	10.20.30.235	16198	88	38 GET / HTTP/1.1 , NTLHSSP_AUTH, User: DIRECTASIA\jeng			
	- 172.17.1.	204 10.10.12.129	HTTP	705	10.20.30.235	16198	80	38 GET / HTTP/1.1			
	_ 172.17.1.	284 10.10.12.129	HTTP	788	10.20.30.235	16198	80	38 GET / HTTP/1.1 , NTLMSSP_NEGOTIATE			
5	_ 172.17.1.	284 10.10.12.129	HTTP	988	10.20.30.235	16198	88	38 GET / HTTP/1.1 , NTLMSSP AUTH, User: \UAT testuser			
	. 172.17.1.	284 10.10.12.129	HTTP	614	10.20.30.235	16198	80	38 GET /ruxitagentjs_ICA275Vfqrux_10185200219132536.js HTTP/1.1			
	_ 172.17.1.	204 10.10.12.129	HTTP	596	10.20.30.235	16198	80	38 GET /assets/marketing.tracking.js HTTP/1.1			
5	_ 172.17.1.	284 10.10.12.129	HTTP	679	10.20.30.235	16198	80	38 GET /assets/marketing.tracking.js HTTP/1.1 , NTLPGSP_NEGOTIATE			
5	. 172.17.1.	284 10.10.12.129	HTTP	1848	10.20.30.235	16198	88	38 GET /assets/marketing.tracking.js HTTP/1.1 , NTLPISSP_AUTH, User: \UAT_testuser			
	. 172.17.1.	204 10.10.12.129	HTTP	857	10.20.30.235	16198	80	38 GET /assets/fonts/Hontserrat/Hontserrat-Regular.ttf HTTP/1.1			
	_ 172.17.1.	204 10.10.12.129	HTTP	940	10.20.30.235	16198	80	38 GET /assets/fonts/Montserrat/Montserrat-Regular.ttf HTTP/1.1 , NTLMSSP_NEGOTIATE			
5	_ 172.17.1.	284 10.10.12.129	HTTP	1140	10.20.30.235	16198	68	38 GET /assets/fonts/Nontserrat/Nontserrat-Regular.ttf HTTP/1.1 , NTLMSSP_AUTH, User: \UAT_te_			
8	. 172.17.1.	284 10.10.12.129	HTTP	1514	10.20.30.235	16198	88	38 POST /rb_bf01663fzw?app=ea7c4b59f27d43eb;end=1 HTTP/1.1 (text/plain)			
	. 172.17.1.	204 10.10.12.129	HTTP	581	10.20.30.235	16218	80	80 GET /assets/lib.js HTTP/1.1			
	_ 172.17.1.	284 10.10.12.129	HTTP	664	10.20.30.235	16218	80	D0 GET /assets/lib.js HTTP/1.1 , NTUHSSP_NEGOTIATE			
5	_ 172.17.1.	284 10.10.12.129	HTTP	921	10.20.30.235	16218	68	80 GET /assets/lib.js HTTP/1.1 , NTLMSSP_AUTH, User: \UAT_testuser			
8	. 172.17.1.	204 10.10.12.129	HTTP	800	10.20.30.235	16218	88	80 GET /assets/image/nav-travel.png HTTP/1.1			
	. 172.17.1.	204 10.10.12.129	HTTP	883	10.20.30.235	16218	80	80 GET /assets/image/nav-travel.png HTTP/1.1 , NTLMSSP_NEGOTIATE			
5	_ 172.17.1.	284 10.10.12.129	HTTP	1083	10.20.30.235	16218	80	D0 GET /assets/image/nav-travel.png HTTP/1.1 , NTUHSSP_AUTH, User: \UAT_testuser			
8	_ 172.17.1.	284 10.10.12.129	HTTP	857	10.20.30.235	16218	88	<pre>B0 GET /assets/fonts/glyphicons-halflings-regular.woff HTTP/1.1</pre>			
8	. 172.17.1.	284 10.10.12.129	HTTP	940	10.20.30.235	16218	80	80 GET /assets/fonts/glyphicons-halflings-regular.woff HTTP/1.1 , NTLMSSP_NEGOTIATE			
	_ 172.17.1.	204 10.10.12.129	NTTP	1140	10.20.30.235	16218	80	B0 GET /assets/fonts/glyphicons-halflings-regular.woff HTTP/1.1 , NTUHSSP AUTH, User: \UAT te_			
	172 17 1	284 18 18 12 129	HTTP	803	10 20 30 235	16218	80	88 GET /assets/image/favicon.32v32 one HTTP/1 1			

\bigotimes Related articles

https://docs.microsoft.com/en-us/iis/configuration/system.webServer/security/authentication/windowsAuthentication/

- Windows Authentication Issue
- Changes required while using Exchange 2019 as HTTPS Real Server
- Decrypt Packet capture with Session keys
- Unable to turn on AG WebUI
- "Session table not valid" Error on AG